SSA-099471: Buffer overflow in Simatic RF Manager

Publishing Date	2013-01-11
Last Update	2013-01-14
Current Version	V1.1
CVSS Overall Score	5.3

Summary:

A buffer overflow exists in a third party module of Simatic RF Manager. This module is an ActiveX component, which will be installed in the user's system when Simatic RF Manager is installed. If a malicious web site is visited with the browser, the attacker will be able to execute arbitrary code in the context of the browser. Siemens provides an update to fix this vulnerability.

AFFECTED PRODUCTS

- RF-MANAGER 2008
- RF-MANAGER Basic v3.0 and lower (as distributed with RF670R and RF640R)

DESCRIPTION

Simatic RF Manager is an engineering and configuration tool for RFID readers like Simatic RF600 from lower layers up to ERP layer and MES layer. The application uses ActiveX for providing various functionalities. These ActiveX components can also be accessed in the context of Microsoft Internet Explorer. So, if a user has installed the Simatic RF Manager's ActiveX applications on his system and visits a web site, code within the ActiveX components can be executed.

One of the ActiveX components is vulnerable to a buffer overflow, so a malicious web site can execute arbitrary code in the browser context and probably take over the whole system.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability Description

A buffer overflow in an ActiveX component can lead to remote code execution in the context of the browser. Depending on the configuration of the affected system, this may be the privileged administrator user. As it is recommended not to use the administrative account for daily work, it is assumed that unprivileged user is affected.

The user has to visit a malicious web site, probably by social engineering like phishing.

CVSS Base Score	6.8
CVSS Temporal Score	5.3
CVSS Overall Score	5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:O/RC:C)

SOLUTION

Siemens provides a software patch for the vulnerability via customer support [1] and recommends installing it as soon as possible.

ADDITIONAL RESOURCES

1. Your customer support can be contacted via this web site:
   http://support.automation.siemens.com/WW/view/en/66829257
2. An overview of the operational guidelines for Industrial Security (with the cell protection concept):
   http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
3. Information about Industrial Security by Siemens:
   http://www.siemens.com/industrialsecurity
4. Recommended security practices by US-CERT:
   http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
5. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
   http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2013-01-11):	Publication Date
V1.1 (2013-01-14):	Corrected wrong CVSS score in header

DISCLAIMER

See: http://www.siemens.com/terms_of_use